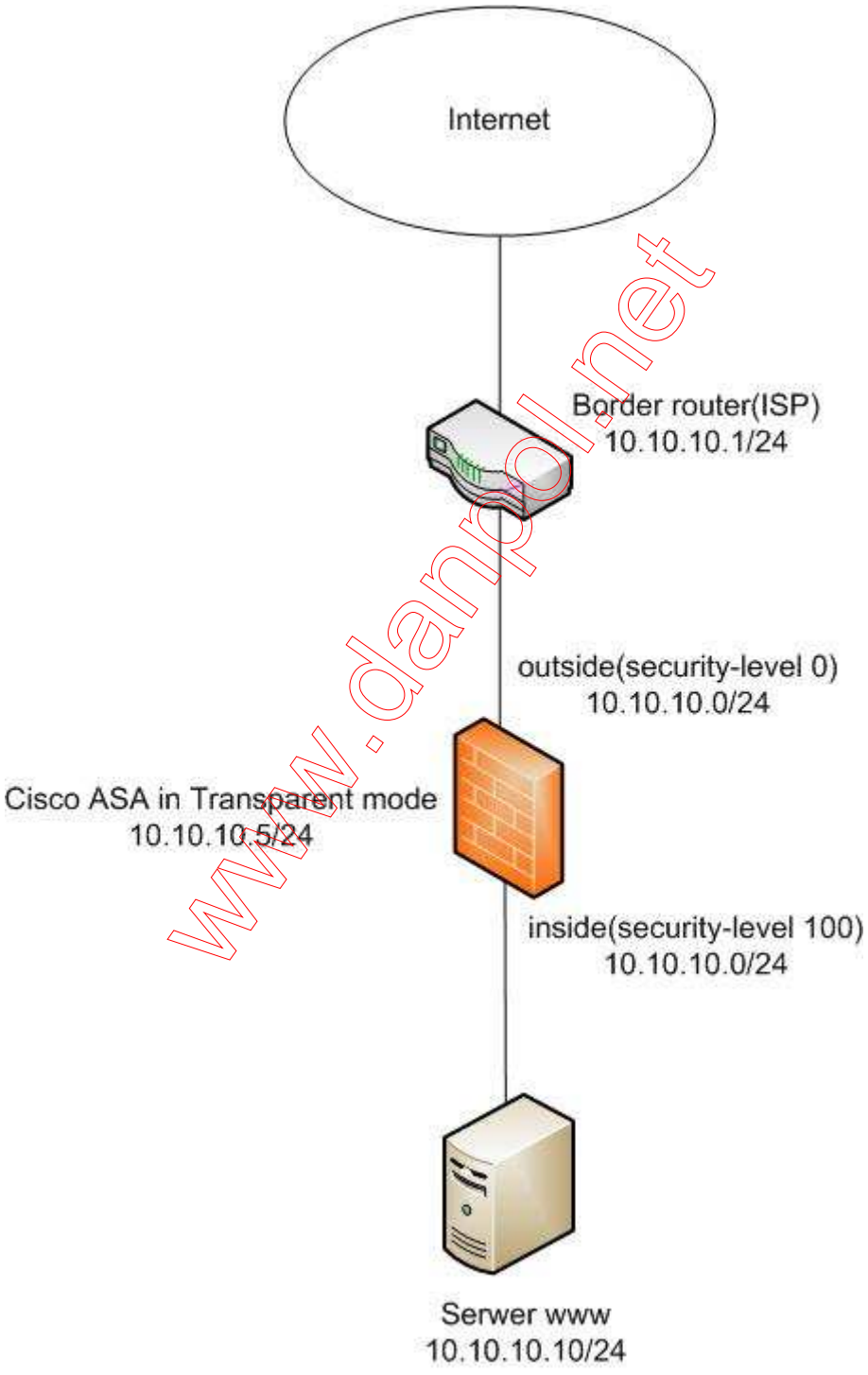
Cisco Asa as a transparent firewall



check your current mode:

show firewall

Firewall mode: Router

- change firewall mode to transparent

(config)# firewall transparent

-verify new mode

ciscoasa(config)# show firewall

Firewall mode: Transparent

- set management ip

ciscoasa(config)# ip address 10.10.10.5 255.255.255.0

- verify management ip

ciscoasa(config)# show ip

Management System IP Address:

ip address 10.10.10.5 255.255.255.0

Management Current IP Address:

ip address 10.10.10.5 255.255.255.0

- set interfaces

ciscoasa(config)#interface ethernet0/0

ciscoasa(config-if)# nameif outside

INFO: Security level for "outside" set to 0 by default.

ciscoasa(config-if)# no shutdown

ciscoasa(config)# interface ethernet 0/1

ciscoasa(config-if)# nameif inside

INFO: Security level for "inside" set to 100 by default.

ciscoasa(config-if)# no shutdown

set default gw for firewall

ciscoasa(config)# route outside 0 0 10.10.10.1

- set logging

ciscoasa(config)# logging on

ciscoasa(config)# logging trap informational

ciscoasa(config)# logging host inside 10.10.10.x

ciscoasa(config)# logging buffered informational

- enable http server or ssh

ciscoasa(config)# http server enable

ciscoasa(config)# http x.x.x.x x.x.x.x outside

- secure asa against arp spoofing by enabling arp inspection on outside interface

ciscoasa(config)# arp outside 10.10.10.1 0023.5eca.74f8

ciscoasa(config)# arp-inspection outside enable

- verify arp-inspection

ciscoasa(config)# show arp-inspection

interface arp-inspection miss

----

outside enabled flood

inside disabled -

- by default firewall in „transparent" mode works similar like in „router" mode but there are some differences ,e.g

ARP is allowed without ACL

You can use only 2 interfaces (outside and inside)

You cannot run any dynamic routing protocols

You cannot use dynamic DNS,

You cannot run IPv6 ,

You cannot use DHCP relay

QoS is unavailable

You can use NAT from 8.0.2 version

VPN termination is unavaible(You can set only site-to-site vpn for ASA managing purposes)

CASE1

-How to allow access to www server on inside interface?

We have to create ACL which allows access to inside server from hosts on outside interface because by default all traffic from zone with security-level 0 to zone with higher security-level are forbidden

access-list outside_access_in remark Serwer www

access-list outside_access_in extended permit tcp any host 10.10.10.10 eq WWW

access-group outside_access_in in interface outside